(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : 0 600 646 A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number : 93309236.3

(51) Int. Cl.[5] : G07F 7/12, G07D 7/00

(22) Date of filing : 19.11.93

(30) Priority : 20.11.92 US 979116

(43) Date of publication of application :
08.06.94 Bulletin 94/23

(84) Designated Contracting States :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant : PITNEY BOWES INC.
World Headquarters
One Elmcroft
Stamford Connecticut 06926-0700 (US)

(72) Inventor : Berson, William
7 Over Rock Lane
Westport, Connecticut 06880 (US)

(74) Representative : Cook, Anthony John et al
D. YOUNG & CO.
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Secure document and method and apparatus for producing and authenticating same.

(57) A document secure against tampering or alteration and method and apparatus for producing and authenticating such a document. A document is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into a label which is the affixed to the document. In one embodiment the signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. This key maybe changed from time to time to increase security. To facilitate authentication the corresponding decryption key is encrypted with another key and incorporated on the card. To validate the document the coded signal is scanned from the label, decoded, decrypted, expanded and displayed. The card may then be authenticated by comparison of the displayed representation of the image and the document.

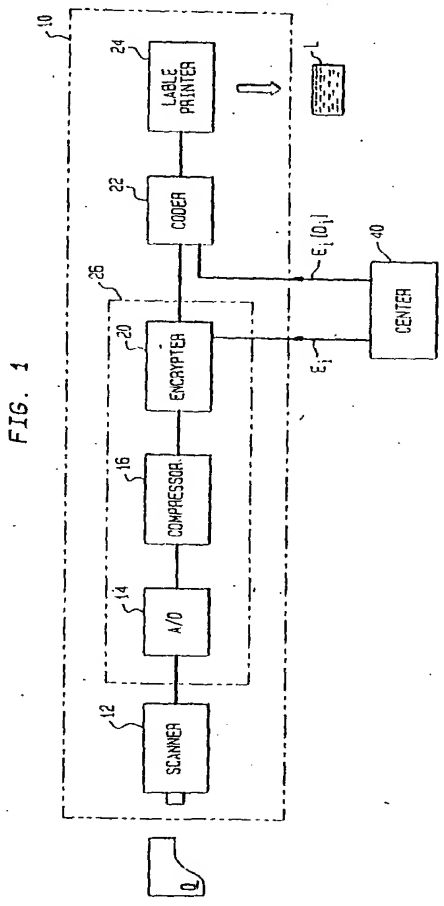


FIG. 1

EP 0 600 646 A2

The subject invention relates to a document or similar item. More particularly, it relates to a document or similar item which has a high degree of security against tampering, and to methods and apparatus for producing and authenticating such documents.

U.S. patent no. 4,853,961; for: "Reliable Document Authentication System", to: Pastor; issued: August 1, 1989, discloses a system wherein a document is authenticated by encryption using a public key encryption system. The invention of the Pastor patent teaches authentication of a document by encryption of information derived from the document, incorporating that encrypted information into the document, recovering the encrypted information from the document and decrypting it, and comparing it to the information as originally included in the document.

While believed to be generally very effective for authenticating documents to detect alteration or tampering, the above described invention suffers from certain disadvantages with existing documents, or documents which are produced to an already defined format. For existing documents it is necessary to input information from the document to create the encrypted information. Typically, this would be done either by manual keyboard input or by some form of character recognition technology. Also, where documents are produced in large numbers to already defined format, e.g. driver's licenses, it is difficult to modify the format to provide for incorporation of the encrypted information in accordance with the Pastor patent.

The above disadvantages of the prior art are overcome in accordance with the subject invention by means of a method and apparatus for producing a secure document and for authenticating that document. Apparatus for producing a secure document includes a scanner for producing a first signal representative of an image of the document. The apparatus further includes an encrypter for encrypting a second signal, which is derived, at least in part, from the first signal, and which includes a representation of the image; and a coder for incorporating a coded representation of the encryption of the second signal onto a label to be affixed to the document.

(As used herein the term "label" preferably describes a conventional label such as an address label. However, it is within the contemplation of the subject invention, and as used herein the term "label" means, any object which may incorporate the coded representation and which can be affixed or otherwise permanently associated with the document.)

Apparatus for authenticating a document so produced includes a reader for reading the coded representation of the second signal from the affixed label, a decoder for decoding the coded representation of the second signal, a decrypter for decrypting the decoded signal, and a display for displaying the representation of the image incorporated in the second signal.

In accordance with the method of the subject invention the document to be secured is scanned to produce the first signal. The second signal, which is derived at least in part from the first signal, and which includes a representation of the image is encrypted and coded and incorporated in the label to be affixed to the document.

Once produced the document is then authenticated by reading the coded representation of the second signal from the affixed label, decoding and decrypting the second signal, and controlling a display in accordance with the decrypted second signal to display the representation of the image which is included in the second signal. The displayed representation of the image and the document are then compared to authenticate the document as free from tampering or attention.

Thus, it is an advantage of the subject invention to provide a method and apparatus for producing a secure document, which are easily applied to existing documents or documents produced in a predefined format.

In accordance with one aspect of the subject invention the first signal is converted into a digital signal for processing.

In accordance with another aspect of the subject invention the second signal includes a compressed form of the first signal.

(Signal compression is well known to those skilled in the art and, in the case of digital signals, involves the application of a predetermined algorithm to a signal to reduce the number of bytes which must transmitted or processed, while still retaining substantially all of the information represented by the signal.)

In accordance with another aspect of the subject invention the second signal is encrypted using an encryption key E_i, for a public key encryption system.

In accordance with still another aspect of the subject invention a decryption key, D_i which correspondences to the key, E_i, is encrypted with a second encryption key, E_1, for the public key encryption system, and the resulting encrypted decryption key $E_1[D_i]$, is appended to the encrypted second signal prior to incorporation of the second signal into the second portion of the document.

In accordance with still another aspect of the subject invention the encrypted second signal is printed on a label as a two dimensional barcode.

In accordance with yet still another aspect of the second invention the apparatus for authenticating the document card stores a decryption key D_i, corresponding to key E_1 and the decryption of the encrypted second signal includes the step of decrypting the encrypted key, $E_1[D_i]$, using the decryption key, D_1, to obtain the decryption key D_i, which may then be

used to decrypt the encrypted second signal.

Thus, it can be seen that the subject invention achieves the above stated advantages by providing a method and apparatus for producing a secure document which includes an image which may be easily compared to document, and which is highly resistant to tampering. Other advantages of the subject invention will be readily apparent to those skilled in the art from consideration of the attached drawings and the detailed description of a preferred, exemplary embodiment set forth below.

In the drawings:

Figure 1 is a schematic block diagram of an apparatus for producing a secure document in accordance with the subject invention.

Figure 2 is a schematic block diagram of an apparatus for authenticating a secure document produced in accordance with the subject invention.

Figure 1 shows a schematic block diagram of apparatus 10 for producing a label L. A document for which the label is intended is scanned by a conventional video scanner 12 to produce a first signal representative of that document D's image. Preferably, the first signal is then converted to a digital form by an analog-to-digital convertor 14 for processing in the digital domain. It is however within the contemplation of the subject invention that at least the signal compression and encryption techniques to be described below may be carried out in the analog domain using signal compression and scrambling technologies well known to those in the analog signal processing arts.

In one embodiment of the subject invention, scanning and compression are done using well known Group III facsimile technology, though other suitable scanning and compression methods are within the contemplation of the subject invention.

The first signal is then input to a compression module 16 where it is compressed to reduce the amount of data which must be stored on label L.

It should be noted that where label L is to have substantially the same form as an address label or the like, data compression is, at the present state of technology, necessary. However, with anticipated improvements in data storage technology, or in applications where the document may comprise a high capacity storage medium (e.g. a floppy disk), it is within the contemplation of the subject invention that the first signal may not require compression but that the full signal may be processed as will be described further below.

Data compression algorithms, for compression of image signals, are known to those skilled in the art. Preferably scanning and signal compression are carried out in accordance with the well known standard for Group III facsimile transmission. Further description of the operation of compressor 16 is not believed necessary to an understanding of the subject invention.

The compressed first signal is then input to an encrypter 20 to be included in the encrypted second signal which will be incorporated into label L as will be described further below. Preferably encrypter 20 encrypts the second signal using an encryption key, E_i, for a public key encryption system such as the well known RSA system.

The encrypted second signal is then encoded in accordance with some predetermined format by coder module 22, which controls code generator 24 to incorporate the encoded encrypted second signal in a portion of document.

In accordance with a preferred embodiment of the subject invention the coded signal is coded as a two dimensional barcode, such as the PDF-417 standard barcode, developed by the Symbol Technology Corporation of New York. However, the encrypted second signal may be coded into any suitable format. For example, for a smart card or a memory card coder 22 and code generator 24 may store the coded second signal as an appropriately formatted binary data block.

In the preferred embodiment where the coded second signal is represented as a two dimensional barcode the barcode will preferably be printed on label L.

In a preferred embodiment of the subject invention compressor module 16, encrypter module 20, and coder module 22 are implemented as software modules in microprocessor 26; which is preferably, an Intel model 80386, or the like, or other microprocessors of greater capacity.

In a preferred embodiment of the subject invention a center 40 transmits encryption code E_i to encrypter module 20. In order to increase the security of label L key E_i maybe changed from time to time. For the highest level of security key E_i maybe changed for each card C produced, or a different key may even be used to encrypt different portions of the second signal.

To facilitate decryption of the second signal in an environment where key E_i is frequently changed center 40 also transmits an encrypted decryption key $E_i[D_i]$ to be appended to the encrypted second signal by coder module 22. Thus, as will be seen below, when document D is to be authenticated the necessary decryption key D_i can be obtained by decrypting $E_i[D_i]$.

Typically, encryption/decryption pair E_i, D_i will remain substantially constant during operation of system 10. However, in applications where system 10 is used to produced labels L for various organizations different pairs E_i D_i may be used for different organizations.

Turning now to Figure 2 apparatus 50 for authenticating a labeled document LD, having label L affixed is shown. The label L of card C is scanned by a barcode scanner 52 having the capability to scan an ap-

propriate two dimensional barcode. The scanned signal is then decoded by decoder module 54 and decrypted by decrypter module 58. In a preferred embodiment of the subject invention decrypter 58 stores decryption key D_i which is used to decrypt encrypted key $E_1[D_i]$ to obtain decryption key D_i. Key D_i is then used to decrypt the decoded signal scanned from label L.

Key D_i is obtained by decrypter 58 from center 40. Typically, D_i will remain constant during operation of system 50, as described above, and a direct communication link between system 50 and center 40 is not necessary and key D_i maybe transmitted in any convenient manner. However, for example, in one application, where label L has a predetermined expiration date it may be desirable to change key D_1 after the expiration date and if such expiration dates occur sufficiently often a direct communication link to center 40 maybe included in system 50.

The decrypted scan signal is then expanded in by an algorithm complimentary to the compression algorithm used in system 10, in a conventional manner which need not be described further for an understanding of the subject invention.

In a preferred embodiment of the subject invention decoder module 54, decrypter module 58, and expander module 60 maybe implemented as software modules in a microprocessor 61.

The decrypted, expanded signal is then displayed by a conventional display 62. The display includes a representation RI of the image of document D. To authenticate labeled document LD it is compared with representation RI. It should be noted that with compression representation RI will be somewhat degraded. It has been found however that using the above described Group III facsimile standard a sufficiently accurate representation of an image of an 8 1/2 x 11 size text document may be coded as approximately 2,000 bytes of data and printed using the above described PDF-417 two dimensional barcode in an area of approximately 3.5 by 2.5 inches. Of course, as described above, with improvements in storage technology and/or the use of media having a higher data storage capacity as embodiments of label L representation RI can be arbitrarily accurately.

The preferred embodiments described above have been given by way of example only, and other embodiments of the subject invention will be apparent to those skilled in the art from consideration of the detailed descriptions set forth above and the attached drawings. Accordingly, limitations on the subject invention are to be found only in the claims set forth below.

Claims

1. A method of producing and authenticating a secure document comprising the steps of:
   a) scanning said document to produce a first signal representative of an image of said at least a portion of said document;
   b) encrypting a second signal, comprising a representation of said image, said second signal being derived at least in part from said first signal;
   c) incorporating a coded representation of said encrypted second signal with said document;
   d) reading said coded representation of said second signal from said document;
   e) decoding said second signal:
   f) decrypting said decoded second signal;
   g) inputting said decrypted second signal to a display to display said representation of said image;
   h) comparing said document to said displayed image to authenticate said document.

2. A method as claimed in claim 1 wherein said second signal comprises a compressed form of said first signal.

3. A method as claimed in claim 1 or claim 2 wherein said second signal is encrypted using an encryption key, E_i, for a public key encryption system.

4. A method as claimed in claim 3 wherein a decryption key, D_i, corresponding to said encryption key, E_i, is encrypted with a second encryption key, E_I, for said public key encryption system.

5. A method as claimed in claim 4 wherein said encrypted decryption key, $E_I[D_i]$, is appended to said encrypted second signal prior to incorporation with said document.

6. A method as claimed in claim 5 wherein said representation of said encrypted second signal is incorporated with said document as a two dimensional barcode.

7. A method as claimed in claim 5 wherein decryption of said encrypted second signal comprises the further steps of decrypting said encrypted key, $E_I[D_i]$ using a decryption key, D_I.

8. A method as claimed in any of claims 2 to 7 wherein said encrypted second signal is incorporated with said document as a two dimensional barcode.

9. A method as claimed in any preceding claim wherein said coded representation is incorporated into a label and said label is affixed to said

document.

10. A method for authenticating a document, said document having a coded representation of an encrypted signal comprising a representation of an image of at least a portion of said document, with said document, comprising the steps of:
    a) reading said coded representation of said signal from said document,
    b) decoding said coded representation of said signal;
    c) decrypting said encrypted representation of said signal; and,
    d) inputting said decrypted representation of said signal to a display for displaying said representation of said image; whereby,
    e) said document may be authenticated by comparison of said document with said displayed representation of said image.

11. A method as claimed in claim 10 wherein said encrypted signal is encrypted using an encryption key, E_t, for a public key encryption system.

12. A method as claimed in claim 11 wherein a decryption key, D_t corresponding to said key E_t, is encrypted with a second encryption key E_t for said public key encryption system to form an encrypted decryption key, $E_t[D_t]$, and said encrypted decryption key, $E_t[D_t]$ is appended to said encrypted signal, and wherein said decryption step further comprises the steps of:
    a) decrypting said encrypted decryption key, $E_t[D_t]$ with a corresponding decryption key, D_t, to recover said decryption key D_t; and,
    b) decrypting said encrypted signal with said key, D_t.

13. Apparatus for authenticating a document, said document having a coded representation of an encrypted signal compressing a representation of a image of at least a portion of said document incorporated with said document, comprising:
    a) means for reading said coded representation of said signal from said document;
    b) decoding means, responsive to said reading means for decoding said coded representation of said signal;
    c) decrypting means, responsive to said decoding means, for decrypting said decoded representation of said signal, and,
    d) display means, responsive to said decrypting means, for displaying said representation of said image: whereby,
    e) said document may be authenticated by comparison of said document with said displayed representation of said image.

14. An apparatus as claimed in claim 13 wherein said encrypted signal is encrypted using an encryption key, E_t, for a public key encryption system.

15. Apparatus as claimed in claim 14 wherein a decryption key, D_t, corresponding to said key E_t, is encrypted with an encryption key E_1 for said public key encryption system to form an encrypted decryption key $E_1[D_t]$, and said encrypted decryption key $E_t[D_t]$ is appended to said encrypted signal, and said decrypting means further comprises:
    a) means for decrypting said encrypted decryption key, $E_1[D_t]$ with a corresponding decryption key, D_t, to recover said decryption key, D_t; and
    b) means for decrypting said encrypted signal using said key, D_t.

16. A document, comprising an encoded representation of an encrypted signal comprising a representation of an image of at least a portion of said document.

17. A document as claimed in claim 16 wherein said digital signal is encrypted using an encryption key, E_t, for a public key encryption system.

18. A document as claimed in claim 17 wherein a decryption key, D_t, corresponding to said encryption key, E_t, is encrypted with a second encryption key, E_1, for said public key encryption system to produce an encrypted description key, $E_t[D_t]$, and said encrypted decryption key, $E_t[D_t]$, is appended to said digital signal prior to incorporation with said document.

19. A document as claimed in claim 16 wherein said representation of said encrypted digital signal is incorporated with said document portion as a two dimensional barcode.

20. A label for securing in, to or in association with an associated document, said label incorporating an encoded representation of an encrypted signal, said signal comprising a representation of an image of said document.

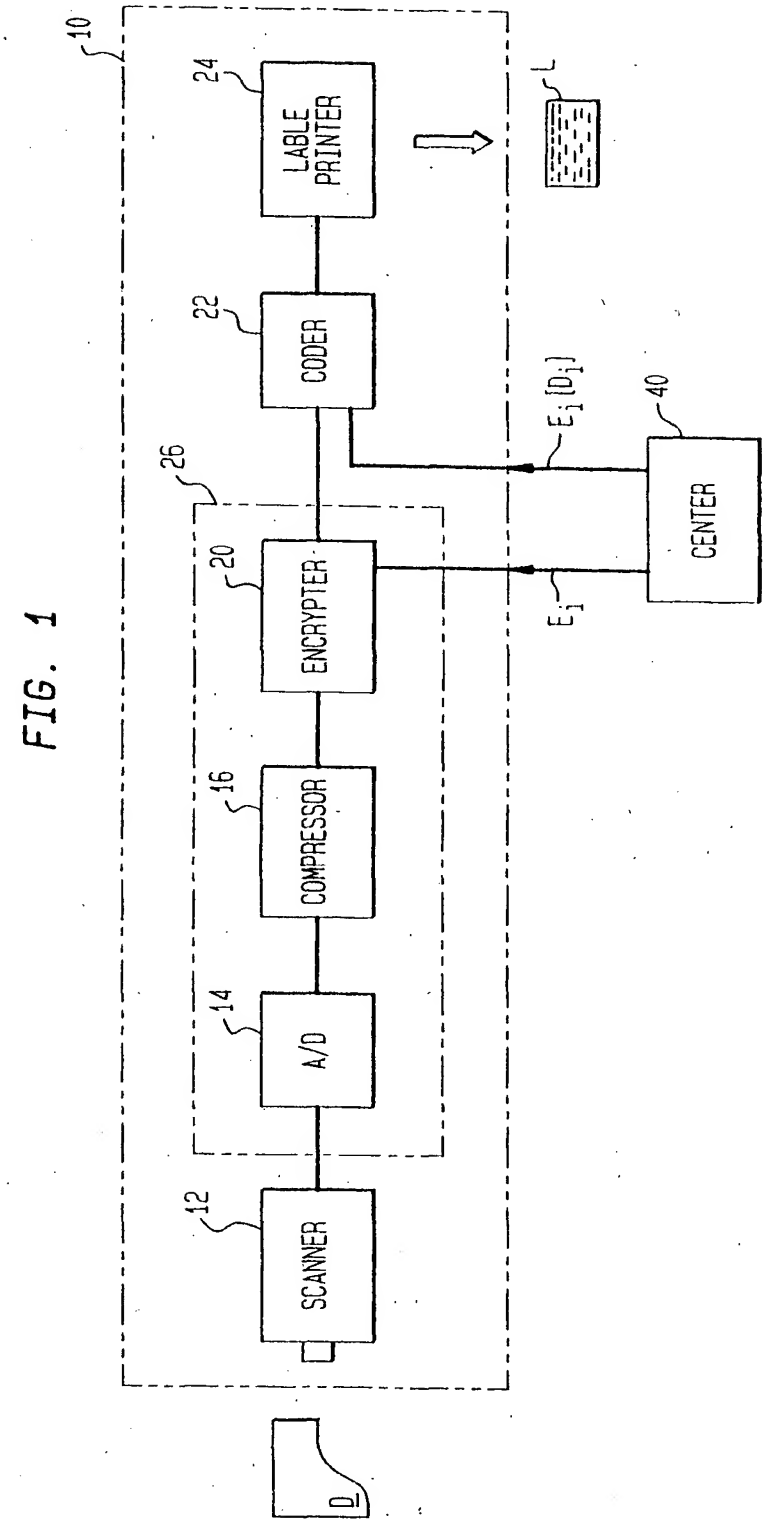
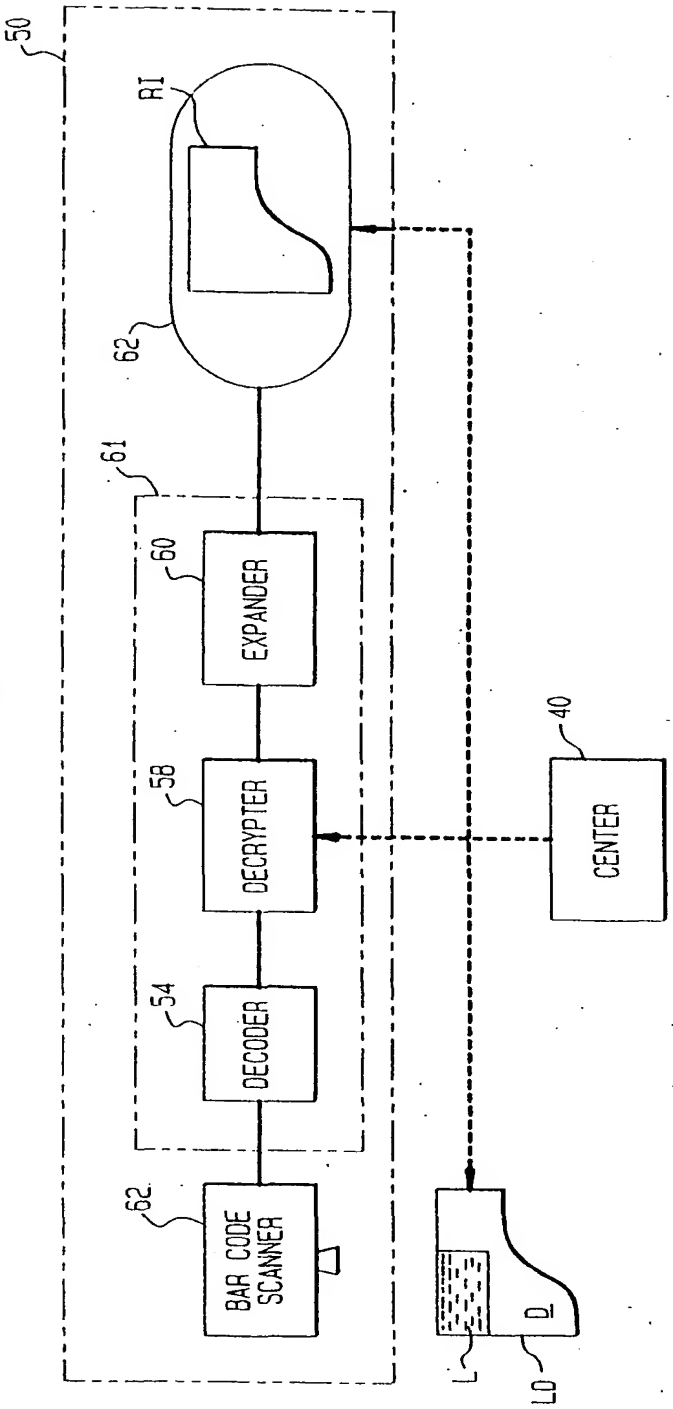


FIG. 1

FIG. 2



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 600 646 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3
05.11.1997 Bulletin 1997/45

(43) Date of publication A2
08.06.1994 Bulletin 1994/23

(21) Application number 93309236.3

(22) Date of filing 19.11.1993

(51) Int Cl.6: G07F 7/12, G07D 7/00, H04N 1/44

(84) Designated Contracting States
DE FR GB NL

(30) Priority: 20.11.1992 US 979116

(71) Applicant: PITNEY BOWES INC.
Stamford Connecticut 06926-0700 (US)

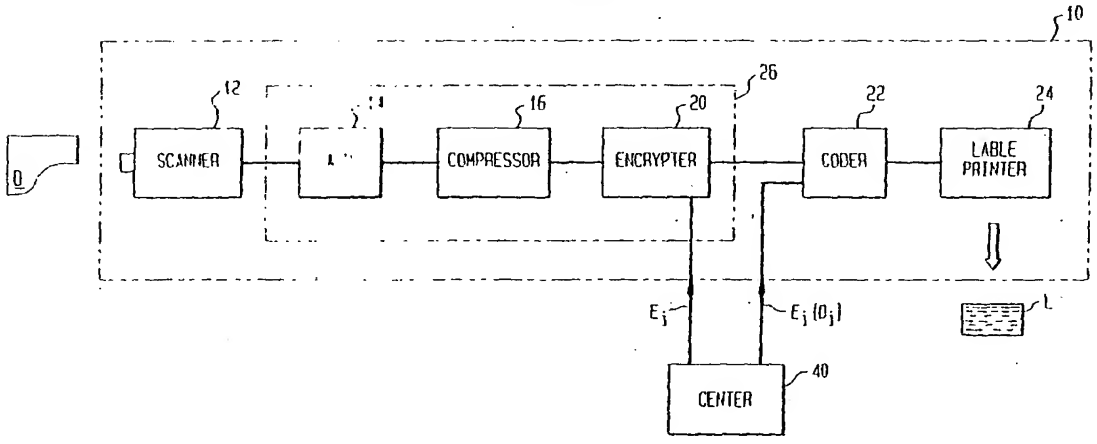
(72) Inventor: Berson, William
Westport, Connecticut 06880 (US)

(74) Representative: Frank, Veit Peter, Dipl.-Ing. et al
Hoffmann Eitle,
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) **Secure document and method and apparatus for producing and authenticating same**

(57) A document secure against tampering or alteration and method and apparatus for producing and authenticating such a document. A document is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding which is incorporated into a label which is the affixed to the document. In one embodiment the signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. This key maybe changed from time to time to increase security. To facilitate authentication the corresponding decryption key is encrypted with another key and incorporated on the card. To validate the document the coded signal is scanned from the label, decoded, decrypted, expanded and displayed. The card may then be authenticated by comparison of the displayed representation of the image and the document.

FIG. 1



EP 0 600 646 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 30 9236

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
X Y	EP 0 286 378 A (LIGHT SIGNATURES INC) 12 October 1988 * the whole document *	1-3,10, 11,13, 14,16,17 4,5,7, 12,15,18	G07F7/12 G07D7/00 H04N1/44
Y	US 4 893 338 A (PASTOR JOSE) 9 January 1990 * the whole document *	4,5,7, 12,15,18	
P,X	US 5 241 600 A (HILLIS W DANIEL) 31 August 1993 * the whole document *	1-3,10, 11,13, 14,16,17	
A	EP 0 334 616 A (LEIGHTON FRANK T ;MICALI SILVIO (US)) 27 September 1989 * abstract; claims; figures *	1-7, 10-18,20	
A	US 5 159 635 A (WANG YNJIUM P) 27 October 1992 * the whole document *	8,19	TECHNICAL FIELDS SEARCHED (Int.Cl.5)
A	US 4 663 622 A (GOLDMAN ROBERT N) 5 May 1987 * abstract; figures 1-16 *	1,2,10, 13,16	G07F G07D H04N G07C
A	EP 0 317 229 A (LIGHT SIGNATURES INC) 24 May 1989		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 September 1997	Guivol, O

EPO FORM 1503 03.82 (P04C01)

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document